ALGEBRAIC COMBINATORICS

Coen del Valle & Colva M. Roney-Dougal

The base size of the symmetric group acting on subsets

Volume 7, issue 4 (2024), p. 959-967.
https://doi.org/10.5802/alco.370

Algebraic Combinatorics is published by The Combinatorics Consortium and is a member of the Centre Mersenne for Open Scientific Publishing
www.tccpublishing.org www.centre-mersenne.org
e-ISSN: 2589-5486

Algebraic Combinatorics
Volume 7, issue 4 (2024), p. 959–967
https://doi.org/10.5802/alco.370

The base size of the symmetric group acting on subsets

Coen del Valle & Colva M. Roney-Dougal

Abstract A base for a permutation group G acting on a set Ω is a subset $\mathcal{B}$ of Ω such that the pointwise stabiliser $G_{(\mathcal{B})}$ is trivial. Let n and r be positive integers with $n > 2r$. The symmetric and alternating groups S_n and A_n admit natural primitive actions on the set of r-element subsets of $\{1, 2, \ldots, n\}$. Building on work of Halasi [8], we provide explicit expressions for the base sizes of all of these actions, and hence determine the base size of all primitive actions of S_n and A_n.

1. Introduction

A *base* for a permutation group G acting on a set Ω is a subset $\{\alpha_1, \alpha_2, \ldots, \alpha_k\} \subseteq \Omega$ with trivial pointwise stabiliser in G. Bases have proved to be tremendously useful in permutation group algorithms (see e.g. [12]); for many computations the complexity is a function of the size of the base used, so it is of interest to find a smallest possible base. The size $b(G)$ of a smallest base for G is called the *base size* of G. Blaha [2] shows that for any positive integer l, and any permutation group G, the problem of determining whether G admits a base of size at most l is NP-complete. On the other hand, there are many different estimates known for $b(G)$ — for example we can derive elementary upper and lower bounds as follows. If $\{\alpha_i\}_{i=1}^k$ is a base for G then any group element $g \in G$ is uniquely determined by the tuple $(\alpha_i^g)_{i=1}^k$ and so $|G| \leqslant |\Omega|^k$. If $k = b(G)$ then $|G_{(\alpha_1,\alpha_2,\ldots,\alpha_i)} : G_{(\alpha_1,\alpha_2,\ldots,\alpha_{i+1})}| \geqslant 2$ for all $1 \leqslant i < k$, so $2^{b(G)} \leqslant |G|$, and hence $(\log|G|)/(\log|\Omega|) \leqslant b(G) \leqslant \log|G|$.

In this paper we consider the primitive faithful actions of the symmetric and alternating groups. A result of Liebeck and Shalev [9] states that there is some absolute constant c such that for $G \in \{\mathrm{S}_n, \mathrm{A}_n\}$ acting primitively, either $b(G) \leqslant c$ or up to equivalence G is acting on either

(i) r-subsets of $[n] := \{1, 2, \ldots, n\}$ with $2r < n$; or
(ii) partitions of $[kl]$ into k parts of size l with $kl = n$.

Manuscript received 8th August 2023, revised 19th March 2024, accepted 20th March 2024.

Keywords. Symmetric group, base size, hypergraph.

Acknowledgements. Research of Coen del Valle is supported by the Natural Sciences and Engineering Research Council of Canada (NSERC), [funding reference number PGSD-577816-2023], as well as a University of St Andrews School of Mathematics and Statistics Scholarship. Both authors thank the referee for their helpful suggestions, which have greatly improved the paper.

Such actions are called *standard*, and most other primitive actions of S_n and A_n are *non-standard*; we denote the permutation groups in case (i) by $\mathrm{S}_{n,r}$ and $\mathrm{A}_{n,r}$, respectively.

In fact, Liebeck and Shalev prove in [9] a stronger result known as the Cameron–Kantor conjecture [7]: any almost simple primitive group either has a base of size at most c (it has since been shown that $c = 7$ is best possible [5, Corollary 1]) or falls into one of three classes of exceptions including the two standard actions of S_n and A_n. In recent years, Burness, Guralnick, and Saxl [4, Corollaries 4 and 5] showed that all non-standard actions of S_n and A_n have base size two or three, and Morris and Spiga [11, Theorems 1.1 and 1.2] gave explicit formulae for all k, l pairs in the actions on partitions, leaving only the actions on subsets to consider.

A 2012 paper of Halasi [8] made progress on the subset action, showing that $b(\mathrm{S}_{n,r}) \geqslant \left\lceil \frac{2n-2}{r+1} \right\rceil$ with equality when $n \geqslant r^2$ — later improved in [6] to $n \geqslant (r^2+r)/2$ — leaving only small n and the action of the alternating group to consider. It is also shown in [8] that $b(\mathrm{S}_{n,r}) \geqslant \lceil \log_2 n \rceil$ for all $n \geqslant 2r$ with equality if $n = 2r$ (at which point the action is imprimitive).

In this paper we completely determine $b(\mathrm{S}_{n,r})$ and $b(\mathrm{A}_{n,r})$. Given $l, k, r \in \mathbb{N}$ set $m_r(l,k) := \frac{1}{k}\left(lr - \sum_{i=1}^{k-1} i\binom{l}{i}\right)$. Our main result is the following.

Theorem 1.1. *Let $n \geqslant 2r$ be fixed and let l be minimal such that there exists some $k \leqslant l+1$ satisfying $0 \leqslant m_r(l,k) \leqslant \binom{l}{k}$ and $\sum_{i=0}^{k-1}\binom{l}{i} + m_r(l,k) \geqslant n$. Then $b(\mathrm{S}_{n,r}) = b(\mathrm{A}_{n+1,r}) = l$.*

Remarks 1.2. A pair (l,k) satisfying the conditions of Theorem 1.1 can be seen to exist by setting $l = n$ and $k = 2$. We give a natural description of the quantity $m_r(l,k)$ at the beginning of Section 3. In the case of the symmetric group, a similar result to Theorem 1.1 was very recently determined independently by Mecenero and Spiga [10] — both their formula and proof take a markedly different form from ours.

Putting together Theorem 1.1, [4, Corollaries 4 and 5, and Remark 7], and [11, Theorems 1.1 and 1.2] the base size of all primitive actions of S_n and A_n are now known.

Corollary 1.3. *All almost simple primitive groups with alternating socle have known base size.*

The complicated statement of Theorem 1.1 is unsurprising, as it needs to interpolate between $\lceil \log_2 n \rceil$ and $\left\lceil \frac{2n-2}{r+1} \right\rceil$. However, when restricting to specific functions n of r, the result can be greatly simplified. Indeed, we deduce Corollary 3.3, which states that $b(\mathrm{S}_{n,r}) = \left\lceil \frac{2n-2}{r+1} \right\rceil$ whenever $n \geqslant (r^2+r)/2$ — recovering the result from [6]. Furthermore, Corollary 3.4 gives an explicit formula for n at least roughly $r^{3/2}$.

As well as the implications in permutation group theory, our results are also of combinatorial interest. Define the *determining number*, $\mathrm{Det}(\Gamma)$, of a graph $\Gamma = (V,E)$ to be the minimum cardinality of a set $S \subseteq V$ such that $\mathrm{Aut}(\Gamma)_{(S)} = 1$. Given positive integers $n \geqslant 2r$, the *Kneser graph*, $K_{n:r}$, has vertex set $V = \{A \subseteq [n] : |A| = r\}$, where sets are adjacent if and only if they are disjoint. Hence, the determining number for $K_{n:r}$ is precisely $b(\mathrm{S}_{n,r})$.

There have been many results in the literature taking this equivalent combinatorial perspective. Indeed, the determining number for Kneser graphs was studied extensively by Boutin [3], dating back to 2006 when she gave early bounds on $\mathrm{Det}(K_{n:r})$, and classified all Kneser graphs with determining number 2, 3, and 4. Additional results, and improvements to these first bounds have been obtained gradually over the following two decades (see [6], for example). In the remainder of this paper we state results only in terms of the group-theoretic formulation, although the results are easily translated.

The structure of the paper is as follows. In Section 2 we set up some general combinatorial machinery, establishing a connection between bases for $\mathrm{S}_{n,r}$ and a class of hypergraphs. In Section 3 we use the tools from Section 2 to prove Theorem 1.1, which we then use to obtain explicit formulae precisely determining the base size for specific functions n of r.

2. Bases and hypergraphs

In this section we translate our problem into the language of hypergraphs. Define $\mathrm{S}_{n,\leqslant r}$ to be the symmetric group S_n acting in the natural way on the set of subsets of $[n]$ of size at most r. Halasi [8] shows that to determine $b(\mathrm{S}_{n,r})$ one may construct a minimum base for $\mathrm{S}_{n,\leqslant r}$.

Lemma 2.1 ([8]). *Fix $n \geqslant 2r$. Then $b(\mathrm{S}_{n,r}) = b(\mathrm{S}_{n,\leqslant r})$.*

To construct a minimum base for $\mathrm{S}_{n,\leqslant r}$ we start with a correspondence lemma which translates our bases into hypergraphs. A *hypergraph* is a pair (V, E) where V is a set of points called *vertices*, and E is a set of subsets of V called *hyperedges*. Given a hypergraph $H = (V, E)$ and $v \in V$, define the H*-neighbourhood* (or *neighbourhood*, when clear from context) of v to be the set

$$N_H(v) := \{e \in E(H) : v \in e\},$$

and the *degree* of v to be $|N_H(V)|$.

Suppose $\mathcal{A}$ is a collection of subsets of $[n]$, each of size at most r. If there are two points $x, y \in [n]$ which are contained in all of the same sets in $\mathcal{A}$, then each element of $\mathcal{A}$ is fixed by the transposition $(x\,y)$, hence $\mathcal{A}$ is not a base for $\mathrm{S}_{n,\leqslant r}$. Similarly if no two such points exist then $\mathcal{A}$ is a base. We call a hypergraph *irrepeating* if all vertices have distinct neighbourhoods. Therefore, a collection $\mathcal{B}$ of distinct subsets of $[n]$ each of size at most r is a base for $\mathrm{S}_{n,r}$ if and only if the pair $([n], \mathcal{B})$ forms an irrepeating hypergraph. We will often take the view that bases *are* hypergraphs, and hence refer to the hypergraph $([n], \mathcal{B})$ simply as $\mathcal{B}$.

If a hypergraph H is irrepeating and has l vertices, n hyperedges (including possibly the empty edge), and maximum vertex degree at most r then we call H an (l, n, r)-*hypergraph*. We call two bases $\mathcal{B}_1, \mathcal{B}_2$ for $\mathrm{S}_{n,\leqslant r}$ *equivalent* if there exists some $\sigma \in \mathrm{S}_{n,\leqslant r}$ with $\mathcal{B}_1^\sigma = \mathcal{B}_2$.

Proposition 2.2. *Fix positive integers l, n, and r, and let $\mathcal{L}$ be the set of isomorphism classes of (l, n, r)-hypergraphs and $\mathcal{S}$ be the set of all equivalence classes of bases of $\mathrm{S}_{n,\leqslant r}$ of size l. Then there exists a one-to-one correspondence $\rho : \mathcal{L} \to \mathcal{S}$.*

The correspondence ρ is via a combinatorial construction known as the *dual hypergraph*. Let H be an irrepeating hypergraph. The *dual* of H, denoted $H^\perp$, is the hypergraph with vertex set identified with the hyperedges of H, and hyperedges identified with vertices of H, where the incidence relations of $H^\perp$ are the reverse of those of H. That is

$$V(H^\perp) := \{v_f : f \in E(H)\},$$

and

$$E(H^\perp) := \{e_u : u \in V(H), v_f \in e_u \iff f \in N_H(u)\}.$$

The proof of Proposition 2.2 requires a couple of easy facts on the operation $\cdot^\perp$ given in the following lemma, which follows directly from the definition.

Lemma 2.3. *Let $\mathcal{H}$ be the space of isomorphism classes of irrepeating hypergraphs. Then $\cdot^{\perp}$ is an involution in* $\mathrm{Sym}(\mathcal{H})$*. Moreover,*

$$|V(H^{\perp})| = |E(H)| \quad \text{and} \quad |E(H^{\perp})| = |V(H)|$$

for all $H \in \mathcal{H}$.

Proof of Proposition 2.2. Let $\mathcal{B}$ be a base for $\mathrm{S}_{n,\leqslant r}$ of size l. By Lemma 2.3, since $\mathcal{B}$ is irrepeating as a hypergraph it has an irrepeating dual, H, say, with l vertices, n edges, and maximum vertex degree at most r. That is, H is an (l,n,r)-hypergraph.

On the other hand, given an (l,n,r)-hypergraph, K, we deduce from Lemma 2.3 that $|V(K^{\perp})| = n$, $|E(K^{\perp})| = l$, and the largest edge of $K^{\perp}$ has size at most r. Moreover, Lemma 2.3 establishes that $K^{\perp}$ is irrepeating and so after relabelling the vertices of $K^{\perp}$ as $1, 2, \ldots, n$, the edges of the resulting hypergraph are indeed a base for $\mathrm{S}_{n,\leqslant r}$ of size l. Therefore, by Lemma 2.3 if we define ρ to return the edge set of the composition of the dual operation, $\cdot^{\perp}$, together with any such relabelling of vertices, then $\rho : \mathcal{L} \to \mathcal{S}$ is a bijection. □

It now follows that to determine the base size of $\mathrm{S}_{n,\leqslant r}$ — and hence, by Lemma 2.1, $\mathrm{S}_{n,r}$ — it suffices to determine the minimum number of vertices of an irrepeating hypergraph with n edges and maximum degree at most r.

A hypergraph is called *k-uniform* if its edge set consists only of edges of size k. A k-uniform hypergraph is called *nearly-regular* if its degree sequence $a_1 \geqslant a_2 \geqslant \cdots \geqslant a_l$ satisfies $a_1 - a_l \leqslant 1$. We use a result of Behrens et al. [1] to prove the final lemma of this section.

Lemma 2.4. *Let k, l, and s be positive integers with $s \leqslant \binom{l}{k}$. Then there exists a nearly-regular k-uniform hypergraph on l vertices with s edges and highest degree $\left\lceil \frac{k}{l} s \right\rceil$.*

Proof. If l divides ks then set $d = l$, otherwise let d be the unique non-negative integer such that $d \left\lceil \frac{k}{l} s \right\rceil + (l-d) \left\lfloor \frac{k}{l} s \right\rfloor = ks$. Consider the sequence $(a_1, a_2, \ldots, a_l)$ where

$$a_i = \begin{cases} \left\lceil \frac{k}{l} s \right\rceil & \text{for } 1 \leqslant i \leqslant d \\ \left\lfloor \frac{k}{l} s \right\rfloor & \text{for } d+1 \leqslant i \leqslant l. \end{cases}$$

From $\binom{l}{k} \geqslant s$, we deduce $\binom{l-1}{k-1} = \frac{k}{l}\binom{l}{k} \geqslant \frac{k}{l} s$, and hence

$$\binom{l-1}{k-1} = \left\lceil \binom{l-1}{k-1} \right\rceil \geqslant \left\lceil \frac{k}{l} s \right\rceil = a_1.$$

Therefore, by [1, Theorem 2.1], there exists a k-uniform hypergraph H with degree sequence $(a_1, a_2, \ldots, a_l)$, so H is nearly-regular with s edges. □

With duality in mind, to construct a small base for $\mathrm{S}_{n,\leqslant r}$ it suffices to build an irrepeating hypergraph with some fixed number of edges, but neighbourhoods as small as possible. A natural way to do this is to successively add a smallest possible edge (in terms of set size), whilst ensuring no two vertices end up with the same neighbourhood. This is precisely how the main result of this section works. Recall $m_r(l,k) = \frac{1}{k}\left(lr - \sum_{i=1}^{k-1} i \binom{l}{i}\right)$ — when clear from context, we omit the subscript r.

Proposition 2.5. *Fix positive integers l, n, and r with $n \geqslant 2r$. Suppose there exists some $k \leqslant l+1$ such that $0 \leqslant m(l,k) \leqslant \binom{l}{k}$, and $\sum_{i=0}^{k-1} \binom{l}{i} + m(l,k) \geqslant n$. Then there exists an (l,n,r)-hypergraph.*

Proof. We construct such a hypergraph. Let H_1 be the unique irrepeating hypergraph on l vertices with all possible edges of size at most $k-1$. By Lemma 2.4, since

$\lfloor m(l,k)\rfloor \leqslant \binom{l}{k}$ there exists some k-uniform hypergraph H_2 on l vertices with exactly $\lfloor m(l,k)\rfloor$ edges, and highest degree at most

$$\left\lceil \frac{k}{l}\left\lfloor \frac{1}{k}\left(lr-\sum_{i=1}^{k-1} i\binom{l}{i}\right)\right\rfloor\right\rceil \leqslant \left\lceil \frac{k}{l}\left(\frac{1}{k}\left(lr-\sum_{i=1}^{k-1} i\binom{l}{i}\right)\right)\right\rceil = r-\sum_{i=1}^{k-1}\binom{l-1}{i-1}.$$

Let H be the irrepeating hypergraph obtained by adding the edges of H_2 to H_1. Then H has l vertices, exactly $\sum_{i=0}^{k-1}\binom{l}{i}+m(l,k)\geqslant n$ edges, and highest degree at most

$$\sum_{i=1}^{k-1}\binom{l-1}{i-1}+\left(r-\sum_{i=1}^{k-1}\binom{l-1}{i-1}\right)=r.$$

By arbitrarily deleting edges of size k until exactly n edges remain we do not increase the degree of any vertex, hence we obtain an (l,n,r)-hypergraph. □

3. Base size of $\mathrm{S}_{n,r}$ and $\mathrm{A}_{n,r}$

In this section we use the tools developed in Section 2 to deduce Theorem 1.1. We then illustrate how the construction works in practice with a brief example, before proving a couple of corollaries.

We first give a description of the quantity $m_r(l,k)$ in terms of bases for $\mathrm{S}_{n,r}$ — it is useful to start by stating the following lemma.

Lemma 3.1. *Let n and r be positive integers with $n\geqslant 2r$, and $\mathcal{B}$ a base for $\mathrm{S}_{n,r}$ with $|\mathcal{B}|=l$. Then $lr=\sum_{x\in[n]}|N_{\mathcal{B}}(x)|$.*

Proof. Count pairs (B,x) where $x\in B\in\mathcal{B}$ in two ways. □

Given a base $\mathcal{B}$ as in the statement of Lemma 3.1 and some positive integer k, set

$$A_1 := \{x\in[n] : |N_{\mathcal{B}}(x)|<k\} \quad\text{and}\quad A_2 := \{x\in[n] : |N_{\mathcal{B}}(x)|\geqslant k\}.$$

We can rewrite the sum in Lemma 3.1 as $lr=\left(\sum_{x\in A_1}|N_{\mathcal{B}}(x)|\right)+\left(\sum_{x\in A_2}|N_{\mathcal{B}}(x)|\right)$, hence

$$\sum_{x\in A_2}|N_{\mathcal{B}}(x)| = lr-\left(\sum_{x\in A_1}|N_{\mathcal{B}}(x)|\right).$$

Since bases are irrepeating, it follows that there are at most $\binom{l}{i}$ distinct neighbourhoods of size i, hence $lr-\left(\sum_{x\in A_1}|N_{\mathcal{B}}(x)|\right)$ is minimally

$$lr-\sum_{i=1}^{k-1} i\binom{l}{i} = km_r(l,k).$$

On the other hand $k|A_2|\leqslant\sum_{x\in A_2}|N_{\mathcal{B}}(x)|$. Therefore $m_r(l,k)$ estimates the minimum number of points of $[n]$ which have $\mathcal{B}$-neighbourhoods of size at least k.

We now proceed with the proof of the symmetric group case of Theorem 1.1.

Proof of Theorem 1.1 for S_n. Let $\mathcal{B}$ be a minimum base for $\mathrm{S}_{n,r}$ so that $b:=b(\mathrm{S}_{n,r})=|\mathcal{B}|$. Let l be minimal satisfying the conditions of Proposition 2.5. Then there exists an (l,n,r)-hypergraph, H, say, and by Proposition 2.2, $\rho(H)$ is a base of size l for $\mathrm{S}_{n,\leqslant r}$. By the minimality of b and Lemma 2.1 we deduce $l\geqslant b$.

Now, let $h\leqslant b+1$ be maximal such that $0\leqslant\left(br-\sum_{i=1}^{h-1} i\binom{b}{i}\right)$ (note h exists since the inequality holds with $h=1<b+1$). It follows from the maximality of h that

$$0\leqslant\frac{1}{h}\left(br-\sum_{i=1}^{h-1} i\binom{b}{i}\right)\leqslant\binom{b}{h}.$$

From Lemma 3.1 and the subsequent discussion we deduce that

$$br \geqslant \left(\sum_{i=0}^{h-1} i\binom{b}{i}\right) + h\left(n - \sum_{i=0}^{h-1}\binom{b}{i}\right),$$

where the second summand describes the fact that any point not contributing to the first summand has neighbourhood of size at least h. Rearranging gives

$$\frac{1}{h}\left(br - \sum_{i=0}^{h-1} i\binom{b}{i}\right) \geqslant n - \sum_{i=0}^{h-1}\binom{b}{i}$$

and so $\sum_{i=0}^{h-1}\binom{b}{i} + m(b,h) \geqslant n$. Thus all conditions of Proposition 2.5 are satisfied. By definition l is the smallest positive integer satisfying the conditions of Proposition 2.5 and so $l \leqslant b$, hence $l = b$ as desired. ☐

We now consider the alternating case.

Proof of Theorem 1.1 for A_n. We prove the result by showing that $b(\mathrm{A}_{n+1,r})$ is equal to $b(\mathrm{S}_{n,r})$. Let $\mathcal{B}$ be a base for $\mathrm{S}_{n,r}$ of size $b(\mathrm{S}_{n,r})$. Consider $\mathcal{B}$ as a collection of r-subsets of $[n+1]$, with $n+1$ having empty neighbourhood. Since $\mathcal{B}$ is a base for $\mathrm{S}_{n,r}$, at most one element of $[n]$ has an empty $\mathcal{B}$-neighbourhood, hence at most two elements of $[n+1]$ do, with all others distinct. But being a base for $\mathrm{A}_{n+1,r}$ is equivalent to having at most two points with equal neighbourhoods, hence $\mathcal{B}$ is a base for $\mathrm{A}_{n+1,r}$ of size $b(\mathrm{S}_{n,r})$. This shows that $b(\mathrm{A}_{n+1,r}) \leqslant b(\mathrm{S}_{n,r})$.

On the other hand, let $\mathcal{C}$ be a base for $\mathrm{A}_{n+1,r}$. If there are two points x and y with the same $\mathcal{C}$-neighbourhood, then assume without loss of generality that x is $n+1$. Let $\mathcal{C}'$ be obtained from $\mathcal{C}$ by deleting $n+1$ from all r-sets in $\mathcal{C}$. Then $\mathcal{C}'$ is a collection of subsets of $[n]$ of size at most r such that each element of $[n]$ has a distinct neighbourhood, that is, a base for $\mathrm{S}_{n,\leqslant r}$. Thus $b(\mathrm{A}_{n+1,r}) \geqslant b(\mathrm{S}_{n,\leqslant r})$, and the result follows from Lemma 2.1. ☐

One can use the proof of the S_n case of Theorem 1.1, together with the proof of [8, Theorem 2.1] to construct a minimum base for $\mathrm{S}_{n,r}$.

Example 3.2. Suppose we wish to construct a minimum base for $\mathrm{S}_{18,7}$. The pair $(l,k) = (5,3)$ satisfies the conditions of Theorem 2.5 with l minimal. Therefore we start by taking the complete graph K_5 adorned with all loops and the empty edge. Following the procedure of the proof we then add the edges of some nearly-regular 3-uniform hypergraph on five points with highest degree at most 2, and exactly two edges. In this case any simple 3-uniform hypergraph with exactly two edges will work, so we may pick one arbitrarily. At this point we have obtained the $(5,18,7)$-hypergraph in Figure 1.

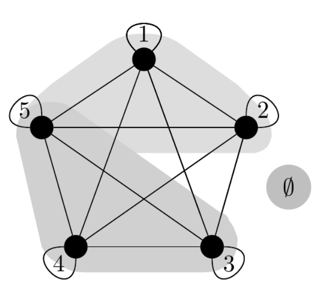

Figure 1. The $(5,18,7)$-hypergraph constructed in Example 3.2, with vertices labelled arbitrarily.

Taking the dual and relabelling the vertices as $1, 2, \ldots, 18$ using the simplicial ordering gives

$$\{\{2,7,8,9,10,17\},\{3,7,11,12,13,17\},\{4,8,11,14,15,18\},\\ \{5,9,12,14,16,18\},\{6,10,13,15,16,17,18\}\}$$

as a minimum base for $\mathrm{S}_{18,\leqslant 7}$ — one can now use Halasi's algorithm in [8] to transform this into a minimum base for $\mathrm{S}_{18,7}$.

In [6] it is shown that $b(\mathrm{S}_{n,r}) = \left\lceil \frac{2n-2}{r+1} \right\rceil$ whenever $n \geqslant (r^2+r)/2$. As a consequence of Theorem 1.1, we can easily obtain an alternate proof of this result.

Corollary 3.3. *Let n and r be positive integers with $n \geqslant (r^2+r)/2$. Then*

$$b(\mathrm{S}_{n,r}) = \left\lceil \frac{2n-2}{r+1} \right\rceil.$$

Proof. First let $n \geqslant (r^2+r+2)/2$. Then $\left\lceil \frac{2n-2}{r+1} \right\rceil \geqslant \frac{2n-2}{r+1} \geqslant r$. Setting $k=2$ and $l = \left\lceil \frac{2n-2}{r+1} \right\rceil$ gives

$$m(l,k) = \frac{1}{2}(lr-l) = \frac{1}{2}\left(\left\lceil \frac{2n-2}{r+1} \right\rceil (r-1)\right) \tag{1}$$

and

$$0 \leqslant \frac{1}{2}\left(\left\lceil \frac{2n-2}{r+1} \right\rceil (r-1)\right) \leqslant \frac{1}{2}\left(\left\lceil \frac{2n-2}{r+1} \right\rceil \left(\left\lceil \frac{2n-2}{r+1} \right\rceil - 1\right)\right) = \binom{l}{k}.$$

Moreover,

$$\begin{aligned} \sum_{i=0}^{k-1} \binom{l}{i} + m(l,k) &= 1 + \left\lceil \frac{2n-2}{r+1} \right\rceil + \frac{1}{2}\left(\left\lceil \frac{2n-2}{r+1} \right\rceil (r-1)\right) && \text{by (1)} \\ &\geqslant 1 + \frac{2}{r+1}(n-1) + \frac{r-1}{r+1}(n-1) \\ &= n. \end{aligned}$$

Therefore, l satisfies the conditions of Theorem 1.1, and hence

$$b(\mathrm{S}_{n,r}) \leqslant \left\lceil \frac{2n-2}{r+1} \right\rceil.$$

Finally, one can construct a base for $n = (r^2+r)/2$ as follows. Our construction yields a base for $\mathrm{S}_{n+1,\leqslant r}$ with exactly one point with empty neighbourhood — by deleting this point and relabelling if necessary we get a base for $\mathrm{S}_{n,\leqslant r}$ of the desired size. We deduce equality from Halasi's lower bound [8, Theorem 3.2]. □

We can continue to use Theorem 1.1 to push even further down, into a range in which no formulae were previously known, although the formula is less pleasant.

Corollary 3.4. *Let n and r be positive integers satisfying $\frac{r^2+r}{2} > n \geqslant r^{3/2} + \frac{r}{2} + 1$. Then*

$$b(\mathrm{S}_{n,r}) = \left\lceil \left(3\left(2n + r - \frac{5}{4}\right) + r^2\right)^{\frac{1}{2}} - r - \frac{3}{2} \right\rceil.$$

Proof. Suppose first that there is some base $\mathcal{B} = \{B_1, \ldots, B_k\}$ for $\mathrm{S}_{n,r}$ with largest vertex neighbourhood of size at most 2. Then B_2 has at least $r-1$ points not in B_1, B_3 has at least $r-2$ points not in $B_1 \cup B_2$, and so on. Thus

$$n \geqslant r + (r-1) + \cdots + 1 = (r^2+r)/2,$$

a contradiction. Therefore, there is no base for $S_{n,r}$ with largest neighbourhood size at most 2. Therefore if $\mathcal{B}$ is any base for $S_{n,r}$ then at least one point has a neighbourhood of size at least three, thus by the discussion following Lemma 3.1, $1+b+\binom{b}{2}+m(b,3) \geqslant n$. That is,

$$n \leqslant 1 + b + \binom{b}{2} + \frac{1}{3}(br - b - b(b-1)) = \frac{b^2 + (2r+3)b}{6} + 1,$$

solving for b (e.g. via the quadratic formula) gives

$$b \geqslant \left(3\left(2n + r - \frac{5}{4}\right) + r^2\right)^{\frac{1}{2}} - r - \frac{3}{2}.$$

The above also shows that if we set l to be (the ceiling of) the quantity above and k to be 3, then l is the minimum positive integer satisfying $1 + l + \binom{l}{2} + m(l,k) \geqslant n$. Therefore, by Theorem 1.1 if we can show that $0 \leqslant m(l,k) = \frac{1}{3}(lr - l^2) \leqslant \binom{l}{3}$, or equivalently that $l \leqslant r \leqslant (l^2 - l)/2 + 1$, then $b(S_{n,r}) = l$.

First, $l > r$ implies $(24n + 4r^2 + 12r - 15)^{1/2} > 4r + 3$. Rearranging gives $n > (r^2 + r + 2)/2$, a contradiction, so $l \leqslant r$. Finally, since $n \geqslant r^{3/2} + \frac{r}{2} + 1$, a straightforward calculation shows that $r \leqslant (l^2 - l)/2 + 1$, hence the result. □

Remark 3.5. In fact, the result holds for $(r^2+r)/2 > n \geqslant \frac{(8r^3+25r^2+4r-28)^{\frac{1}{2}}}{6} + \frac{r}{2} + 1$ — the lower bound of $n \geqslant r^{3/2} + \frac{r}{2} + 1$ is used in the statement simply for presentation.

One could continue to play this game, obtaining explicit formulae for different ranges of n, however the calculations quickly become increasingly complicated.

References

[1] Sarah Behrens, Catherine Erbes, Michael Ferrara, Stephen G. Hartke, Benjamin Reiniger, Hannah Spinoza, and Charles Tomlinson, *New results on degree sequences of uniform hypergraphs*, Electron. J. Combin. **20** (2013), no. 4, article no. 14 (18 pages), https://doi.org/10.37236/3414.

[2] Kenneth D. Blaha, *Minimum bases for permutation groups: the greedy approximation*, J. Algorithms **13** (1992), no. 2, 297–306, https://doi.org/10.1016/0196-6774(92)90020-D.

[3] Debra L. Boutin, *Identifying graph automorphisms using determining sets*, Electron. J. Combin. **13** (2006), no. 1, article no. 78 (12 pages), https://doi.org/10.37236/1104.

[4] Timothy C. Burness, Robert M. Guralnick, and Jan Saxl, *On base sizes for symmetric groups*, Bull. Lond. Math. Soc. **43** (2011), no. 2, 386–391, https://doi.org/10.1112/blms/bdq123.

[5] Timothy C. Burness, Martin W. Liebeck, and Aner Shalev, *Base sizes for simple groups and a conjecture of Cameron*, Proc. Lond. Math. Soc. (3) **98** (2009), no. 1, 116–162, https://doi.org/10.1112/plms/pdn024.

[6] José Cáceres, Delia Garijo, Antonio González, Alberto Márquez, and María Luz Puertas, *The determining number of Kneser graphs*, Discrete Math. Theor. Comput. Sci. **15** (2013), no. 1, 1–14, https://doi.org/10.46298/dmtcs.634.

[7] Peter J. Cameron and William M. Kantor, *Random permutations: some group-theoretic aspects*, Combin. Probab. Comput. **2** (1993), no. 3, 257–262, https://doi.org/10.1017/S0963548300000651.

[8] Zoltán Halasi, *On the base size for the symmetric group acting on subsets*, Studia Sci. Math. Hungar. **49** (2012), no. 4, 492–500, https://doi.org/10.1556/SScMath.49.2012.4.1222.

[9] Martin W. Liebeck and Aner Shalev, *Simple groups, permutation groups, and probability*, J. Amer. Math. Soc. **12** (1999), no. 2, 497–520, https://doi.org/10.1090/S0894-0347-99-00288-X.

[10] Giovanni Mecenero and Pablo Spiga, *A formula for the base size of the symmetric group in its action on subsets*, Australas. J. Combin. **88** (2024), no. 2, 244–255.

[11] Joy Morris and Pablo Spiga, *On the base size of the symmetric and the alternating group acting on partitions*, J. Algebra **587** (2021), 569–593, https://doi.org/10.1016/j.jalgebra.2021.08.009.

[12] Ákos Seress, *Permutation group algorithms*, Cambridge Tracts in Mathematics, vol. 152, Cambridge University Press, Cambridge, 2003, https://doi.org/10.1017/CBO9780511546549.

Coen del Valle, School of Mathematics and Statistics, University of St Andrews, St Andrews, UK
E-mail : cdv1@st-andrews.ac.uk

Colva M. Roney-Dougal, School of Mathematics and Statistics, University of St Andrews, St Andrews, UK
E-mail : Colva.Roney-Dougal@st-andrews.ac.uk